IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA v. AHMAD 'UMAR AGHA (a/k/a "THE PRO") & FIRAS DARDAR (a/k/a "THE SHADOW"), Defendants.	Criminal No. 1:14-MJ-292 **UNDER SEAL**

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT AND ARREST WARRANTS

I, Patrick DiMauro, being first duly sworn, hereby depose and state the following:

BACKGROUND AND OVERVIEW OF THE CONSPIRACY

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) assigned to the Washington Field Office, Washington, D.C. I have been employed by the FBI as a Special Agent for three years. Throughout my FBI employment, I have received training in general law enforcement and in specialized areas including national security computer intrusions. As a Special Agent of the FBI, I am authorized to investigate crimes involving computer intrusion, national security, and other crimes stated under federal law, including Title 18 of the United States Code.

2. I make this affidavit in support of an application for a criminal complaint charging AHMAD 'UMAR AGHA (also known as "THE PRO" and "AHMED TEMER AGGA") and FIRAS DARDAR (also known as "THE SHADOW") with conspiring to violate numerous federal laws as prohibited by 18 U.S.C. § 371. As described in more detail below, AGHA and DARDAR knowingly and willfully conspired to violate 18 U.S.C. §§ 1028(a)(3), 1029(a)(3), 1030(a)(2)(C), 1030(a)(5)(A), 1030(a)(5)(B), 1038, 2701, and 2387.

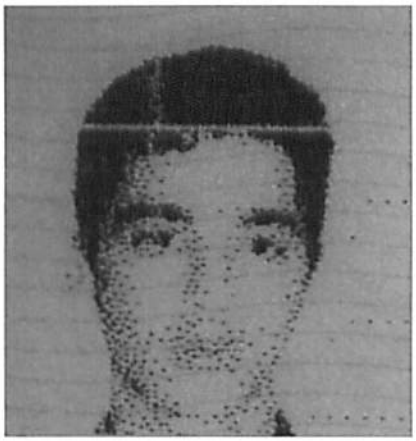
3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Because this affidavit is for the limited purpose of establishing probable cause for a criminal complaint, it does not set forth every fact learned in the course of this investigation.

The Defendants

4. Defendants AHMAD 'UMAR AGHA and FIRAS DARDAR are members of a Conspiracy that refers to itself as the "SYRIAN ELECTRONIC ARMY" or "SEA." AGHA is a resident of Damascus, Syria. DARDAR is a resident of Homs, Syria.

A. This is an image of AGHA:

B. This is an image of DARDAR:



5. AGHA and DARDAR have obtained passwords for private and public electronic mail (email) accounts, conducted computer intrusion attacks, altered websites without authorization, and issued messages and conducted interviews on behalf of the Conspiracy.

Manner and Means of the Conspiracy

6. The primary method of the Conspiracy for infiltrating computer systems to further its unlawful goals can be summarized as follows:

A. A member of the Conspiracy obtains email addresses for persons associated with a target entity.

B. A member of the Conspiracy sends a phishing[1] email purporting to be from a trusted source that contains a link to a website which appears to be a trusted website but is actually controlled by the Conspiracy.

---

[1] "Phishing" is the act of attempting to acquire information, such as usernames and passwords, by masquerading as a trustworthy entity in an electronic communication. "Spearphishing" consists of "phishing" attempts directed at specific individuals or companies. Attackers may gather personal information about their target to increase their likelihood of success.

C. Any user that clicks on the link is asked for credentials, such as a username and password, for a legitimate system. For the attacks that were successful, at least one user provided their credentials to the Conspiracy.

D. The legitimate credentials are then used without authorization by a member of the Conspiracy to access the computer systems of the target entity.

E. Once the computer systems are accessed, a member of the Conspiracy redirects legitimate traffic, defaces and alters text, sends messages using the victim's accounts, attempts further phishing attempts, or engages in other illegitimate activities.

Summary of the Conspiracy's Unlawful Activities

7. The Conspiracy targeted individuals and organizations in the United States and elsewhere, some of which were perceived by the Conspiracy as antagonistic toward the Syrian government. The targeted individuals and entities include, but are not limited to, the following:

A. In September 2011, a member of the Conspiracy altered the Harvard University website homepage and substituted an image of Syrian President Bashar al-Assad with a message saying "Syrian Electronic Army Were Here."

B. In October 2011, a member of the Conspiracy, using the credentials of an actual employee of the Washington Post, a daily newspaper based in Washington, D.C., accessed, without authorization, a computer server used by the Washington Post and created a false web post on live.washingtonpost.com.

C. In October 2011, a member of the Conspiracy used LinkedIn.com (a social networking website specifically targeting professionals) to send an email to a person who had previously worked in the Executive Office of the President (EOP), an office in the executive branch overseen by the White House Chief of Staff which, according to the

White House's website, traditionally has housed many of the President's closest advisors. A member of the Conspiracy used a particular Hotmail account requesting a LinkedIn "connection." If the recipient of the email clicked on a link provided within the email, it would have allowed the member of the Conspiracy to view that person's profile and work associates. The attempt was unsuccessful.

D. In June 2012, multiple emails were sent by a member of the Conspiracy from the accounts whitehouse-online@hotmail.com and whitehouse_online@hotmail.com to employees of the Executive Office of the President. These emails contained links to sites controlled by the Conspiracy. These attempted infiltrations of the computer systems of EOP were unsuccessful.

E. In August 2012, the Conspiracy compromised the Twitter account of the Reuters news agency, an international news organization that is based in London, United Kingdom. Tweets were sent with false information on the conflict in Syria. At approximately the same time, the Reuters news website was compromised by the Conspiracy and a false report was posted to a Reuters journalist's blog.

F. In February 2013, a member of the Conspiracy sent emails to the email accounts of at least two employees of the Washington Post, whose email servers were at that time located in the Eastern District of Virginia. The email appeared to contain a link to a statement from the Government of Qatar, but actually contained a link to a website controlled by a member of the Conspiracy. At least one Washington Post employee clicked on the link and, as a result, the Conspiracy obtained the username and password for at least one actual employee.

G. In March 2013, a member of the Conspiracy sent an email to multiple employees of Human Rights Watch (HRW), a non-governmental organization dedicated to protecting and defending human rights and headquartered in New York, New York. The email appeared to contain a link to a press release from the Government of Qatar, but actually contained a link to a website controlled by a member of the Conspiracy. Multiple employees of HRW clicked on the link. Using the malicious website, the Conspiracy obtained usernames and passwords for multiple HRW employees. A member of the Conspiracy used an actual HRW employee's username and password to access, without authorization, the HRW website and post messages criticizing HRW's reports related to Syria.

H. In April 2013, a member of the Conspiracy used a compromised email account to send emails to employees of National Public Radio (NPR), a non-profit membership media organization that serves as a national syndicator to a network of approximately 900 public radio stations in the United States, including numerous stations in the Eastern District of Virginia.[2] The email contained a link that appeared to resolve to an Office of the United Nations High Commissioner for Refugees (UNHCR) report related to Syria, but actually resolved to a website controlled by the Conspiracy. The UNCHR is an office within the United Nations that is mandated to lead and coordinate international action to protect refugees. Numerous employees of NPR clicked on the link, which prompted them to enter their usernames and passwords. A member of the

[2] Those stations include but are not limited to WCVE (Chesterfield, VA); WHRG (Norfolk, VA); WHRG (Norfolk, VA); WHRO (Norfolk, VA); WHRX (Norfolk, VA); WNSB (Norfolk, VA); and WQIQ (Spotsylvania, VA).

Conspiracy used compromised usernames and passwords of actual NPR employees to send additional phishing emails. In addition, a member of the Conspiracy used compromised credentials to access, without authorization, the NPR website and deface multiple news stories.

I. In April 2013, a member of the Conspiracy sent an email to employees of the Associated Press, a multinational non-profit news agency headquartered in New York, New York, which appeared to come from a well-known international organization. At least one employee of the Associated Press clicked on a malicious link in the email. Using credentials obtained from at least one employee of the Associated Press, a member of the Conspiracy accessed the Associated Press Twitter account, without authorization, and sent a message from that account falsely claiming the White House had been bombed and United States President Barack Obama injured.

J. In May 2013, a member of the Conspiracy sent an email from a compromised email account to employees of CNN, which is a subsidiary of Turner Broadcasting System, Inc., a media conglomerate that is owned by TimeWarner, Inc., and headquartered in Atlanta, Georgia. The email contained a link that appeared to resolve to a media website, but actually resolved to a website controlled by the Conspiracy. Dozens of employees of CNN clicked on the link and entered their credentials, which were then obtained by the Conspiracy.

K. In May 2013, a member of the Conspiracy sent an email containing a link to what appeared to be a news article to employees of The Onion, a Chicago, Illinois, organization that produces satirical content regarding international, national, and local news. The email purported to be from an email account associated with an actual

employee of the UNHCR and appeared to have been sent from the UNHCR.org server. Through this fraudulent email, the Conspiracy obtained at least one set of log-in credentials for the servers used by The Onion for email. Using a set of authentic credentials, a member of the Conspiracy accessed, without authorization, an email account for an actual employee of The Onion and sent an email to The Onion staff containing what appeared to be a link to a news article. Once again, in response to this fraudulent email, at least two employees of The Onion clicked on the false link and provided their authentic credentials directly to the Conspiracy. One of The Onion users had administrative access to the electronic accounts of The Onion. Using this user's authentic credentials, a member of the Conspiracy altered, without authorization, the account passwords and other information for both that user's email account and The Onion's Twitter accounts. A member of the Conspiracy accessed, without authorization, the Twitter accounts of The Onion and posted false information on the accounts.

L. In May 2013, a member of the Conspiracy obtained login credentials, through a spearphishing attack, to the Twitter account of E! Online, an online portal of E!, which is an American basic cable and satellite network that is owned by NBCUniversal, Inc., a corporation headquartered in New York, New York. The Conspiracy then altered, without authorization, the Twitter account by posting false messages about the Syrian conflict to E! Online's Twitter feed.

M. In July 2013, a member of the Conspiracy created an email account that appeared to be associated with an employee of the EOP (VICTIM 1). The member of the Conspiracy sent emails from this account to the personal and work emails for several EOP employees. The emails contained links which appeared to resolve to media

websites, but actually pointed to websites which were controlled by the Conspiracy. At least one of the current employees of the EOP (VICTIM 2) clicked on a link and provided actual email credentials to the Conspiracy through the fraudulent website. A member of the Conspiracy thereafter accessed, without authorization, VICTIM 2's personal email account and used that account to send emails to other EOP employees, at least one of which requested the password to a White House social media account. No official EOP email account was successfully compromised, despite the efforts of the Conspiracy.

N. In July 2013, a member of the Conspiracy compromised the website of the Daily Dot, an online news website headquartered in Austin, Texas. The Conspiracy altered, without authorization, the website with images related to Syria and deleted a legitimate article about Syria.

O. In August 2013, a member of the Conspiracy sent emails that appeared to be from the Chief Executive Officer of Outbrain, Inc., to numerous employees of that company, which offers a content recommendation service whose online widget presents links to content in order to help Internet publishers increase web traffic at their websites. These emails contained a link that appeared to resolve to a media website but actually pointed to a website controlled by the Conspiracy. At least one employee of Outbrain clicked on the link and provided their actual email credentials to the Conspiracy through the fraudulent website. The Conspiracy used credentials harvested from the spearphishing attack to obtain unauthorized access to Outbrain's advertising controls. Using those controls, the Conspiracy was able to redirect web traffic for a number of Outbrain's customers including CNN, The Washington Post, and Time.

P. In August 2013, a member of the Conspiracy created an email account that appeared to belong to the Chief Executive Officer of Chartbeat, Inc., a real-time analytics service used by Internet companies with headquarters in New York, New York, and data servers in Ashburn, Virginia, within the Eastern District of Virginia. A member of the Conspiracy used the account to send emails to Chartbeat employees. These emails contained a link that appeared to resolve to a media website but actually pointed to a website controlled by the Conspiracy. At least one employee of Chartbeat (VICTIM 3) clicked on the link and provided actual email credentials to the Conspiracy through the fraudulent website. The Conspiracy used credentials harvested from the spearphishing attack to obtain access to Chartbeat's Internet web services, Chartbeat client information, and to post messages on the Chartbeat Twitter account.

Q. In August 2013, a member of the Conspiracy sent emails to employees of USA Today, a national daily newspaper, and its parent, Gannett News Corporation, from two separate email accounts. These accounts appeared to be from domains associated with USA Today and the Gannett Corporation, both of which are headquartered in McLean, Virginia, within the Eastern District of Virginia. The emails contained a link that appeared to resolve to a media website, but actually resolved to a website controlled by the Conspiracy.

R. In August 2013, a member of the Conspiracy sent numerous emails to employees of Melbourne IT, an Australian company that provides Internet-based technology services. The emails appeared to come from the Chief Executive Officer of Melbourne IT. The emails contained a link that appeared to resolve to a media website, but actually resolved to a website controlled by the Conspiracy. At least two employees

of Melbourne IT clicked on the link and entered their Melbourne IT credentials. These employees had the ability to change Domain Name System (DNS) tables within Melbourne IT's systems. A DNS table is a table that correlates domain names (such as nytimes.com) with the Internet Protocol address of a specific computer. A member of the Conspiracy accessed, without authorization, Melbourne IT's systems and used the harvested credentials to redirect numerous domains to a website controlled by the Conspiracy. The domain names redirected included huffingtonpost.co.uk and nytimes.com.

S. In August 2013, a member of the Conspiracy launched a spearphishing attack to obtain the login credentials for multiple Twitter accounts at the New York Post, a daily newspaper in New York City that is owned by News Corp, a multi-national corporation headquartered in New York, New York. The Conspiracy defaced, without authorization, the Twitter accounts by posting pro-Syrian government messages to the Twitter feeds.

T. In September 2013, a member of the Conspiracy created an email account that appeared to belong to the Chief Executive Officer of J. Walter Thompson, Inc., an advertising agency based in New York, New York. A member of the Conspiracy sent an email from the account to another JWT employee (VICTIM 4). The email contained a link that appeared to resolve to a media website, but actually resolved to a website controlled by the Conspiracy. VICTIM 4 clicked on the link and entered email credentials. Using VICTIM 4's compromised account, a member of the Conspiracy made a request to reset VICTIM 4's password on another Internet account, and that account controlled the registration information for the domain Marines.com.

Marines.com is an Internet website operated on behalf of the United States Marine Corps Recruiting Command, which is headquartered in Quantico, Virginia, in the Eastern District of Virginia. Using the compromised Internet account, a member of the Conspiracy redirected, without authorization, the domain Marines.com to a web page controlled by the Conspiracy.

U. In September 2013, a member of the Conspiracy sent an email appearing to originate from an employee of the National Aeronautics and Space Administration (NASA), a United States government agency that is responsible for the civilian space program, as well as aerospace and aeronautic research and development, to multiple email addresses associated with real persons associated with NASA facilities, including Langley Research Center in Hampton, Virginia, which is in the Eastern District of Virginia. Several NASA employees clicked on the link provided by a member of the Conspiracy but any attempted access was stopped by NASA network security devices.

V. In November 2013, a member of the Conspiracy obtained, through a spearphishing attack, the email and Twitter credentials of a filmmaker who was critical of the Syrian government. Without authorization, the Conspiracy defaced the individual's website and Twitter account, and obtained copies of personal correspondence.

W. In November 2013, a member of the Conspiracy obtained, through a spearphishing attack, the login credentials of an employee of Time, a weekly newsmagazine. Without authorization, the Conspiracy defaced the magazine's Twitter account and an online poll.

X. In November 2013, a member of the Conspiracy obtained, through a spearphishing attack, the login credentials for multiple employees of Vice, an online

magazine headquartered in New York, New York. The Conspiracy defaced Vice's website and redirected Vice's website to a website controlled by the Conspiracy. Vice.com, the website of Vice, is hosted on a server located within the Eastern District of Virginia.

Y. In January 2014, a member of the Conspiracy obtained, through a spearphishing attack, the login credentials for multiple employees of the Microsoft Corporation, a technology company headquartered in Redmond, Washington. Without authorization, the Conspiracy defaced a blog and Twitter account operated by Microsoft, and obtained copies of electronic communications.

The Unlawful Objects of the Conspiracy

8. In conducting the malicious computer activities summarized above and described in more detail below, members of the Conspiracy, including AGHA and DARDAR, conspired to violate numerous federal statutes. Those statutes include:

A. 18 U.S.C. § 1028(a)(3) (knowingly possess with intent to use unlawfully or transfer unlawfully five or more authentication features);

B. 18 U.S.C. § 1029(a)(3) (knowingly and with intent to defraud possess fifteen or more devices which are counterfeit or unauthorized access devices);

C. 18 U.S.C. § 1030(a)(2)(C) (intentionally access a computer without authorization or exceed unauthorized access, and therefore obtain information from any protected computer);

D. 18 U.S.C. § 1030(a)(5)(A) (knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, causing loss aggregating at

least $5000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer and causing damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security);

E. 18 U.S.C. § 1030(a)(5)(B) (intentionally access a protected computer without authorization, and as a result of such conduct, recklessly cause damage);

F. 18 U.S.C. § 2701 (intentionally access without authorization a facility through which an electronic communication is provided or intentionally exceed an authorization to access that facility, and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system);

G. 18 U.S.C. § 1038 (engage in conduct with the intent to convey false or misleading information under circumstances where such information may reasonably be believed and where such information indicates that an activity has taken, is taking, or will take place that would constitute a violation of chapter 113B of Title 18); and

H. 18 U.S.C. § 2387 (advise, counsel, urge, or cause - or attempt to cause - insubordination, disloyalty, mutiny, or refusal of duty by any member of the military or naval forces of the United States, with the intent to interfere with, impair, or influence the loyalty, morale, or discipline of the military or naval forces of the United States).

PROBABLE CAUSE

The Conspiracy Begins and Targets the Washington Post

9. On November 11, 2010, a member of the Conspiracy created the email account th3pr0123@gmail.com. Search warrant returns from that email account indicate the account was created using IP Address 82.137.248.2,[3] which public databases indicate is registered to Syrian Telecommunications Establishment ("Syrian Telecom"). The person registering the account also provided a specific SMS number.[4] This email account was used to receive stolen credentials from victims, to register domains used by the Conspiracy, and to communicate with co-conspirators.

10. Based on records obtained from search warrants served on this account, the primary user of this account was AGHA, a/k/a "The Pro." On April 28, 2013, an email was sent from th3pr0123@gmail.com to another email account. Attached to the email were two images, both of which appeared to depict an identification document. The image on the identification document appeared to be the same person depicted in Paragraph 4(A). The name on the identification document was Ahmad 'Umar AGHA. Additional images of the same individual were sent from the account to the same account (*i.e.*, the user sent the images to himself) on April 6, 2013. These images appear to depict a wedding, and the individual in the photos appears to be the same individual on the identification document. Emails sent to the account by others address the recipient as "Ahmed" and "Ahmed Temer Agga." Finally, an April 14, 2013,

[3] An Internet Protocol Address (IP Address) is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication.

[4] SMS stands for "Short Messaging Service," which is a widely-used application for sending text messages via cellular phone.

an online communication between th3pr0123@gmail.com and sea.the.shadow@gmail.com seized pursuant to a search warrant indicates that the user of this account, identified as "The Pro," forwarded the contents of an email related to the registration of a domain used by the Conspiracy to the user of the sea.the.shadow@gmail.com account. In the email, The Pro is addressed as "Ahmad Temer Agga."

11. On August 24, 2011, a member of the Conspiracy created an account, "theprosea," on the website LinkedIn.com. Search warrant returns from LinkedIn indicate that the member of the Conspiracy used the IP address 82.137.248.3 at Syrian Telecom and the email address th3pr0123@gmail.com to register the account. The LinkedIn search warrant returns also included communications sent from the targeted LinkedIn account. A member of the Conspiracy later used this LinkedIn account to attempt to contact a potential spearphishing target.

12. On October 19, 2011, a member of the Conspiracy used the authentic credentials for a Washington Post employee to access, without authorization, computer servers used by the Washington Post for its live.washingtonpost.com website. Based on interviews with employees of the Washington Post, a member of the Conspiracy created a false posting on the website, which stated "Hacked by Syrian Electronic Army" and credited "Th3 Pro." The Information Technology staff of the Washington Post identified IP addresses used by the Conspiracy in the attack as: 76.73.101.180, 82.137.248.3, 82.137.248.4, 82.137.248.5, 82.137.248.6, and 91.144.18.219. All but the first of these addresses were registered to Syrian Telecom.

13. The IP addresses used to conduct the defacement of the Washington Post were used at other times by members of the Conspiracy. For instance, search warrant returns for the e-mail account th3pr0123@gmail.com indicate that between April 20, 2012 and June 4, 2012, the IP address 82.137.248.5 was used on 137 occasions to access the th3pr0123@gmail.com

account. The IP address 82.137.248.3 was used to log into "theprosea" LinkedIn account approximately 70 times between October 2011 and February 2013, and the IP address 82.137.248.5 was used to log into the same LinkedIn account more than 50 times in that time period.

14. On April 21, 2012, a member of the Conspiracy created the email account seatheshadow@gmail.com. Search warrant returns from that email account indicate the account was created using IP Address 178.52.134.163, which public databases indicate is registered to Syrian Telecom. The person registering the account also provided a specific SMS number. The account sea.the.shadow@gmail.com is listed as an alternate username for the account. Between July 7, 2012, and December 26, 2013, the user of this account and the user of th3pr0123@gmail.com exchanged approximately 218 email communications that concerned the hacking activities of the Conspiracy.

15. Based on records obtained from search warrants served on this account, the primary user of this account was DARDAR, a/k/a "The Shadow." On November 2, 2013, the user of sea.the.shadow@gmail.com sent two emails to another user. The first email was signed "The Shadow" and attached to the email were images of an identification document. The identification document depicted the person shown in Paragraph 4(B), and included a name which translates to "FIRAS DRDR." The second email contained an attachment which appears to be a document issued by the Syrian Ministry of the Interior. It bears the name FERAS DARDAR and includes personal information about that individual. Correspondence sent to the account addresses the recipient as "FERAS DARDAR" and "FIRAS NOUR ALDEN DARDAR." Finally, in an interview with a journalist that was conducted via email in May of 2013, the user of th3pr0123@gmail.com identified the user of sea.the.shadow@gmail.com as

"THE SHADOW" and described THE SHADOW as a hacker in the SEA "special operations department."

The Conspiracy Phishes Employees of the Executive Office of the President

16. On October 4, 2011, a member of the Conspiracy used LinkedIn to send an email to the personal email account of an employee of the EOP (VICTIM 2). The email requested that the EOP employee make a "connection" with the member of the Conspiracy. When two LinkedIn users make a "connection," each user can view the other user's profile, as well as all the other persons who have "connections" with that user.

17. Search warrant returns for the email account th3pr0123@gmail.com indicate that on February 24, 2012, a member of the Conspiracy using a computer that was logged into that email account conducted two Internet searches via Google.com for the terms "eop.gov webmail."

18. Records from Microsoft indicate that at approximately 8:00 p.m. on June 4, 2012, a member of the Conspiracy using the IP address 82.137.248.5 (which was used in the Conspiracy's defacement of The Washington Post) created the email account whitehouse_online@hotmail.com. The member of the Conspiracy creating the account listed his first name as "Whitehouse.gov." That same day, a member of the Conspiracy using a computer assigned the IP address 78.46.142.27 created the account whitehouse-online@hotmail.com. The individual creating the email account listed his first name as "WhiteHouse.gov."

19. On the evening of June 4, 2012, multiple emails were sent by a member of the Conspiracy from the account whitehouse_online@hotmail.com to employees of the EOP. The first such email was sent approximately one to two hours after the creation of the whitehouse_online@hotmail.com account. The subject line of the emails sent from the account was "Replacement login information for [user's email address] at The White House." Because

the user of the account had used a first name of "Whitehouse.gov," the emails appeared to have been sent from "Whitehouse.gov." The body of the emails contained a request for the user to reset a password. The email stated that the recipient could change his or her password by clicking on a link provided in the text of the email, and then entering the recipient's login credentials. The link appeared to be a link to the whitehouse.gov domain. In fact, the link directed any user who clicked on it to http://78.46.142.27/~WH/.

20. Also on June 4, 2012, multiple emails were sent from the account whitehouse-online@hotmail.com to employees of the EOP. The first such email was sent approximately five minutes after the creation of the whitehouse-online@hotmail.com account. The emails were identical to those sent from the whitehouse_online@hotmail.com account.

21. In June 2012, the computer assigned IP address 78.46.142.27 was used to host several web pages, including one located at http://78.46.142.27/~syrian/. The webpage contained images of the Syrian flag and a link using the words "Th3 Pr0" at the bottom of the page. A link on the webpage led to the domain blog.thepro.sy. Moreover, between June 1, 2012 and June 24, 2012, the IP address 78.46.142.27 was used to access the "theprosea" LinkedIn account four times. The same IP address was also used to log into the email account th3pr0123@gmail.com four times in June 2012.

22. No employees of the Executive Office of the President clicked on the malicious links contained in the spearphishing emails in June 2012.

The Conspiracy Continues to Create Infrastructure and Research Potential Victims

23. According to search warrant results obtained from Google, on October 22, 2012, a member of the Conspiracy using a computer that was logged into the email account th3pr0123@gmail.com conducted multiple Internet searches via Google.com for the terms

"outlook web access eop.gov," "owa eop.gov," and "storm.eop.gov." An Internet search of "storm.eop.gov" returns results indicating that "storm.eop.gov" is a domain associated with an email server used by the White House.

24. On January 25, 2013, a member of the Conspiracy created the email account leakssyrianesorg@gmail.com. Records from Google indicate the Google account was created from IP Address 62.212.72.240, which is registered to Syrian Telecom. This account was a secondary account associated with th3pr0123@gmail.com and the username was entered as "SEA leaks." The account also listed the same SMS contact number as the th3pr0123@gmail.com account.

The Conspiracy Targets the Washington Post Again

25. On February 20, 2013, a member of the Conspiracy, using a computer that was logged into the email account th3pr0123@gmail.com, conducted multiple Internet searches via Google.com for the terms "thepost-cp.washpost.com." "wash post webmail." and "washpost webmail."

26. On February 20, 2013, emails were sent by a member of the Conspiracy from the email account mos-office@mofa.gov.qa to at least two employees of The Washington Post. The email address mos-office@mofa.gov.qa appears to be a legitimate email address that was compromised by the Conspiracy. The website Qatar-leaks.com, which bears the logo of the Syrian Electronic Army, allows any visitor to the page to access multiple emails sent to and from that email account. The emails sent to the Washington Post from the mos-office@mofa.gov.qa email address were addressed to "Washingtonpost" and appeared to contain a link to a press release from the Ministry of Foreign Affairs of Qatar. The link actually directed the targets of the attack to websites which prompted the targets to provide their username and password; the

two websites used in the emails were hosted by net23.net, which is controlled by 000webhost.com, with links of "http://secureids.washpost.net23.net/nidp/sam12/sso.washpost?id=143&sid=1&option=credential&sid=1&uid=631&pre=auto" and "http://webmail.washpost.net23.net/owa/auth/logon.aspx?replaceCurrent=1&url=https%3a%2f%2fwebmail.washpost.com%2fowa%2f".

27. On February 22, 2013, a member of the Conspiracy received the authentic credentials for VICTIM 6, an employee of The Washington Post, by means of an automated email from 000webhost.com. The email was sent to the email account th3pr0123@gmail.com and contained VICTIM 6's username and password.

The Conspiracy Targets Additional Media Organizations and Human Rights Groups, Including National Public Radio and Human Rights Watch

28. On March 16, 2013, a member of the Conspiracy, using a computer that was logged into the email account th3pr0123@gmail.com, conducted multiple Internet searches via Google.com for the terms "@hrw.org email contact" and "@npr.org media email." Hrw.org is the domain name for Human Rights Watch (HRW), an organization that has been critical of the Syrian government. Npr.org is the domain name for National Public Radio, a media organization that has reported on the conflict in Syria.

29. On March 17, 2013, an email was sent by a member of the Conspiracy from the email account mos-office@mofa.gov.qa to multiple employees at HRW. The email, addressed to "HRW employees," appeared to be a link to a press release from the Ministry of Foreign Affairs of Qatar. The link actually directed the targets of the attack to a website which prompted

the targets to provide their username and password. The website was hosted on a site that was a subsidiary of 000webhost.com: mail.hrw.net84.net.

30. Search warrant returns from the email account th3pr0123@gmail.com indicate that, between March 17, 2013, and March 18, 2013, a member of the Conspiracy received seven emails from an automated email account. The emails were sent from a server hosted on 000webhost.com and appeared to contain the credentials of HRW employees. The body of each email began with the acronym "HRW" and then listed the username and password of a HRW employee. For instance, on March 17, 2013, a member of the Conspiracy received the authentic credentials for VICTIM 7, VICTIM 8, and VICTIM 9, actual employees of HRW, by means of automated emails from a server hosted on 000webhost.com.

31. Based on information provided by HRW, a member of the Conspiracy then sent additional phishing emails to other HRW employees from a legitimate HRW.org email account. Additional employees clicked on the phishing link and entered their credentials. The Conspiracy also attempted to use HRW email accounts to phish other persons. A review by HRW uncovered that one compromised HRW email account was used by the Conspiracy to send more than 6,000 additional phishing emails, mostly targeting media organizations.

32. On March 17, 2013, a member of the Conspiracy used authentic credentials provided by HRW employees to access, without authorization, HRW's website and post multiple messages, including:

Syrian Electronic Army Was Here

All Your reports are FALSE !!

The defacements were automatically posted to HRW's Twitter account. Based on information provided by HRW, the IP address used to commit the defacement was 46.17.103.125, which is registered in Russia.

33. The IP address assigned to the computer that was used to deface the HRW website was also used at other times by the Conspiracy. Between February 13, 2013, and May 16, 2013, that same IP address was used on nine occasions by a member of the Conspiracy to access the th3pr0123@gmail.com account. Between February 17, 2013, and March 4, 2013, the IP address was used to log into "theprosea" LinkedIn account 13 times. Records from Twitter also indicate that the IP address was used to create a Twitter account associated with the Conspiracy, "@SEA_Official3". In addition, that IP address was used in the Conspiracy's defacement of The Onion.

34. On March 17, 2013, at 10:56 and 10:57 pm EST, the Twitter account for "OFFICIAL_SEA" posted two screen captures of the defacement of the HRW's website.

35. On March 20, 2013, a member of the Conspiracy using the account th3pr0123@gmail.com conducted searches via Google.com for the terms "https://webmail.washingtonpost.com," "washington post media emails," "washington post emails," "washpost media contacts," "washpost emails," "webmail.washpost.com," "@washpost.com email," and "@washpost.com." The member of the Conspiracy also clicked on "http://www.washingtonpostads.com/contact-us-directory".

36. On March 20, 2013, a member of the Conspiracy using a computer logged into the account th3pr0123@gmail.com conducted a search using Google.com for "hrw.org iraq" and then clicked on "http://www.hrw.org/middle-eastn-africa/iraq".

37. On March 22, 2013, a member of the Conspiracy using a computer logged into the account th3pr0123@gmail.com conducted searches using Google.com for "hrw logo."

38. On March 25, 2013, a member of the Conspiracy using a computer logged into the account th3pr0123@gmail.com clicked on http://www.hrw.org/bios/kenneth-roth and conducted a search using Google.com for "hrw profile."

39. On April 15, 2013, a member of the Conspiracy received a test phishing email in the email account th3pr0123@gmail.com from an email account using the domain unhcr.org. The test phishing email had the subject line "UNHCR Report – Syria" and was signed with the name of a real person at the UNHCR.

40. On April 15, 2013, an email appearing to be sent from a real person from UNHCR, which was substantially the same as the test phishing email, was sent by a member of the Conspiracy to multiple NPR employees with the subject line "UNHCR Report – Syria." The body of the email contained what appeared to be a link to a UNHCR report about Syria. However, the link actually directed the targets of the attack to a website associated with the Conspiracy that prompted the targets to provide their username and password.

41. On April 15, 2013, a member of the Conspiracy received more than 40 emails at the account th3pr0123@gmail.com from an automatic email address that appeared to contain usernames and passwords for NPR employees. The body of each email began with the acronym "NPR" and then listed a username and password. On April 15, 2013, for example, a member of the Conspiracy received the authentic credentials for VICTIM 10, VICTIM 11, and VICTIM 12, actual employees of NPR, by means of automated emails from SOUL.WEBSITEWELCOME.COM, which was associated with a false webpage created by the Conspiracy.

42. On April 15, 2013, a member of the Conspiracy used the authentic credentials provided by NPR employees to access, without authorization, and take over multiple NPR employees' email accounts. From those compromised email accounts, a member of the Conspiracy sent phishing emails to other NPR employees. The body of the phishing emails contained what appeared to be a link to a Washington Post article about the bombing of the Boston Marathon in 2013. However, the link actually directed the targets of the attack to a website associated with the Conspiracy that prompted the targets to provide their username and password.

43. On April 16, 2013, a member of the Conspiracy used the authentic credentials provided by a NPR employee to access, without authorization, NPR's website data and deface multiple news stories with the words "Syrian Electronic Army Was Here." The same day, a member of the Conspiracy used the authentic credentials provided by NPR employees to access, without authorization, and take over multiple NPR Twitter accounts. After accessing NPR Twitter accounts, the Conspiracy changed the passwords. A member of the Conspiracy received an automatic message from Twitter to confirm that the contact email address for the Twitter account @TellMeMoreNPR, which is associated with NPR's program "Tell Me More," was changed to th3p.r0123@gmail.com.

44. Based on my training and experience, I know that Google email accounts do not recognize a period in an email address. Thus, the email account th3p.r0123@gmail.com is the same account as th3pr0123@gmail.com.

45. On April 16, 2013, a member of the Conspiracy, using a computer that was logged into the email account th3pr0123@gmail.com, conducted multiple Internet searches for the NPR Tech Team via Google.com. The same day, a member of the Conspiracy received an

automatic message from Twitter to confirm that the contact email address for the Twitter account @NPRTechTeam was changed to th3p.r0123@gmail.com.

46. On April 16, 2013, a member of the Conspiracy received an automatic message from Twitter to confirm that the email address for the Twitter account associated with NPR's Science Desk was changed to sea.the.shadow@gmail.com.

47. On April 16, 2013, the Twitter account for "@OFFICIAL_SEA" sent two tweets claiming credit for hacking NPR's official website and Twitter accounts.

The Conspiracy Targets the Associated Press

48. On April 23, 2013, a member of the Conspiracy sent an email with a malicious link to multiple employees of the Associated Press. The email was sent from a compromised UNHCR account, and thus the email came from the legitimate UNHCR.org domain.

49. On April 23, 2013, a member of the Conspiracy received the authentic credentials for VICTIM 13, an employee of the Associated Press, by means of an automated email from 000webhost.com, which was associated with a false webpage created by the Conspiracy.

50. On April 23, 2013, the IP Address 46.57.135.14 was used by a member of the Conspiracy to access, without authorization, the webmail portal of the Associated Press. That same day, the same IP address was used by a member of the Conspiracy to access the th3pr0123@gmail.com account 39 times. Records from Twitter indicate the same IP address was also used on April 23, 2013, to access Twitter accounts "@Th3Pr0_SEA" and "@OFFICIAL_SEA," which are associated with the Conspiracy.

51. On April 23, 2013, a member of the Conspiracy received an automated message from Twitter at the email account th3pr0123@gmail.com to confirm a password reset for the Twitter account "@AP," which belongs to the Associated Press.

52. On April 23, 2013, a member of the Conspiracy accessed the Associated Press Twitter account, without authorization, and sent a message from that account falsely claiming the White House had been bombed and United States President Barack Obama injured.

The Conspiracy Attacks The Onion

53. On May 4, 2013, a member of the Conspiracy sent an email with a subject line of "theonion" from the account sea.the.shadow@gmail.com to the account th3pr0123@gmail.com containing a list of over twenty-five email addresses with a domain of theonion.com.

54. On May 4, 2013, a member of the Conspiracy sent an email to employees of The Onion containing a link to what appeared to be a news article. The email purported to be from an email account associated with an actual employee of the UNHCR, and appeared to have been sent from the UNHCR.org server. When an employee clicked on the link in the email it directed the employee to a website that requested the employee's email credentials. Through this fraudulent email, the Conspiracy obtained at least one set of authentic log-in credentials for the servers used by The Onion for email.

55. On May 5, 2013, a member of the Conspiracy received the authentic credentials for VICTIM 14, an employee of The Onion, by means of two automated emails from 000webhost.com, which was associated with a false webpage created by the Conspiracy.

56. On May 6, 2013, a member of the Conspiracy logged into the email account for VICTIM 14, an actual employee of The Onion, and sent an email, without authorization, impersonating that employee to The Onion staff containing what appeared to be a link to a news article. Once the employees clicked on the link they were redirected to a website that mimicked The Onion's email website and requested the employees' authentic log-in credentials. At least

four employees of The Onion clicked on the false link and provided their authentic credentials directly to the Conspiracy.

57. On May 6, 2013, a member of the Conspiracy received the authentic credentials for VICTIM 14, VICTIM 15, VICTIM 16, and VICTIM 17, employees of The Onion, by means of automated emails from 000webhost.com, which was associated with a false webpage created by the Conspiracy.

58. On May 6, 2013, a member of the Conspiracy, using authentic log-in credentials obtained from an employee of The Onion, accessed, without authorization, the Google Apps servers used by The Onion.

59. As a result of the Conspiracy gaining access to The Onion's accounts with Google on the morning of May 6, 2013, the staff of The Onion advised their employees at approximately 11:48 AM Eastern Time on that day to reset their passwords and emailed them a link for that purpose.

60. On May 6, 2013, a member of the Conspiracy used the compromised email account of one of The Onion employees, without authorization, in order to send a duplicate email to the email from 11:48 AM Eastern Time but with a modified link that would redirect the user to another site. At least two employees of The Onion clicked on this false link and provided their credentials directly to the Conspiracy.

61. On May 6, 2013, a member of the Conspiracy received the authentic credentials for VICTIM 18 and VICTIM 19, employees of The Onion, by means of automated emails from 000webhost.com, which was associated with a false webpage created by the Conspiracy.

62. One of The Onion users that clicked on a false link provided by the Conspiracy had administrative access to the electronic accounts of The Onion. Using this user's authentic

credentials, a member of the Conspiracy altered, without authorization, the account passwords and other information for both that user's email account and The Onion's Twitter accounts on May 6, 2013.

63. On May 6, 2013, a member of the Conspiracy accessed, without authorization, the Twitter accounts of The Onion from IP Address 46.17.103.125 and posted false information on the account. That same day, a member of the Conspiracy using the Firefox Internet browser accessed the Google Apps server used by The Onion without authorization from the IP Address 46.17.103.125. The same IP address had been used on attacks on HRW.

64. On May 6, 2013, a member of the Conspiracy changed, without authorization, the email address associated with The Onion Twitter account, "@TheOnion." An email confirming this change was sent to email address th3pr0123+onion@gmail.com. Based on my training and experience, Twitter will ignore all characters in an email address after the character "+". Thus, an email sent by Twitter to the account th3pr0123+onion@gmail.com will actually direct emails to the account th3pr0123@gmail.com.

65. On May 6, 2013, a member of the Conspiracy changed, without authorization, the email address associated with The Onion News Network Twitter account, "@ONN." An email confirming this change was sent to email address th3pr0123+onion3@gmail.com.

66. On May 6, 2013, a member of the Conspiracy using the Firefox Internet browser accessed the Google Apps server used by The Onion, without authorization, from the IP Address 46.17.103.125.

67. On May 6, 2013, a member of the Conspiracy accessed a Twitter account controlled by The Onion, without authorization, and sent false messages purporting to be from The Onion.

68. Members of the Conspiracy then searched for articles about their activities. On May 6, 2013, a member of the Conspiracy who was logged into the th3pr0123@gmail.com account reviewed the following Internet news stories:

A. http://news.cnet.com/8301-1023_3-57583142-93/onions-twitter -account-hacked-by-syrian-electronic army/;

B. http://www.heavy.com/news/2013/05/the-onion-twitter-hacked-by-syrian-electronic-army/; and

C. http://www.philly.com/philly/blogs/trending/The-Onion-hacked-on-Twitter-Facebook-Syrian-Electronic-Army.html.

69. On May 7, 2013, a member of the Conspiracy who was logged into the th3pr0123@gmail.com account searched on Google.com for items associated with "Satirical news website The Onion's Twitter page was hacked by a hacker called Th3 Pr0's Syrian Electronic Army." The user then clicked on the following link: http://news.cnet.com/8301-1023_3-57583142-93/onions-twitter -account-hacked-by-syrian-electronic army/. The user later did a search on Google.com for "After hacking into the Onion's Twitter account earlier today, members of the Syrian Electronic Army confirmed."

70. On May 8, 2013, a member of the Conspiracy who was logged into the th3pr0123@gmail.com account clicked on the Internet news article "http://security .cbronline.com/news/Syrian-electronic-army-hacks-the-onions-twitter-accoiunts-080513."

The Conspiracy Targets CNN

71. Between March 21, 2013, and April 18, 2013, a member of the Conspiracy using the account th3pr0123@gmail.com conducted more than thirty searches via Google.com that related to CNN, CNN's employees, and CNN's email and information technology systems.

72. On May 14, 2013, an employee of CNN received an email sent by a member of the Conspiracy from a compromised email account. The email was sent from a domain belonging to a media organization. The email contained a link which appeared to resolve to a news article. However, the link actually resolved to http://blog.conservatives.com/wp=content/uploads/cnn.php.

73. On May 20, 2013, another CNN employee received an email from a different compromised email account using a legitimate media organization's domain sent by a member of the Conspiracy. The subject of the email was "news" and the email contained a link which appeared to resolve to a news article. However, the link actually resolved to http://www.ikhwansuez.net/cnn.php. Multiple employees of CNN clicked on the link and entered their credentials.

74. On May 20, 2013, yet another CNN employee received an email from a different compromised email account. The subject of the email was "news" and the email contained a link which appeared to resolve to a media website. However, the link actually resolved to http://www.ikhwansuez.net/cnn.php. Clicking on the link directed users to a webpage designed to mimic a web-based email login page. In all, dozens of CNN employees received phishing emails.

75. On May 20, 2013, a member of the Conspiracy sent an email from the account sea.the.shadow@gmail.com to the account th3pr0123@gmail.com. The email contained a list of usernames at CNN.

The Conspiracy Targets the Executive Office of the President Again

76. On July 26, 2013, VICTIM 1, among others at EOP, received an email in a personal email account from an email account purporting to belong to VICTIM 5. The email

account was "[NAME OF VICTIM 5]@mc.internetmailserver.net". The email contained a link which appeared to resolve to a media website. However, the link actually resolved to http://www.klchr-pshr.com/bo.php.

77. On July 27, 2013, VICTIM 2, who previously received a request for a "connection" on LinkedIn from a member of the Conspiracy, received an email in a personal email account that appeared to come from VICTIM 1's personal email account but was actually sent by a member of the Conspiracy. The email contained a link that appeared to resolve to a media website. However, the link actually resolved to http://www.klchr-pshr.com/bo.php. VICTIM 2 clicked on the link in the email, which directed VICTIM 2 to enter personal email login credentials. VICTIM 2 entered the email login credentials for a personal email account.

78. Login data from VICTIM 2's personal email account indicates that on July 27, 2013, a member of the Conspiracy accessed, without authorization, the personal email account of VICTIM 2 using a computer assigned the IP address 188.139.245.9. That IP address resolves to Syria.

79. On July 27, 2013, a member of the Conspiracy changed the account settings for VICTIM 2's personal email account to add a forwarding address. The forwarding address added was leaks.syrianes.org@gmail.com. The email account leaks.syrianes.org@gmail.com was listed as a secondary account for the email address of th3pr0123@gmail.com.

80. On July 27, 2013, a member of the Conspiracy sent email from VICTIM 2's personal email account to other EOP employees. At least two of the emails requested the password to a White House social media account (no such password was provided). A number of the fraudulent emails contained a link which appeared to resolve to a media website.

However, the link actually resolved to http://www.gloryshipsghana.com/wh.php. No EOP account was successfully compromised by the Conspiracy.

The Conspiracy Targets Media Organizations Through Third Party Vendors

81. On August 14, 2013, a member of the Conspiracy sent emails that appeared to be from the Chief Executive Officer of Outbrain, Inc., to numerous Outbrain employees. These emails contained a link that appeared to resolve to a media website but actually pointed to "http://centriplant-dev.coreware.co.uk/wp-content/blogs.dir/ob.php." At least one employee of Outbrain clicked on the link and provided actual email credentials to the Conspiracy through the fraudulent website.

82. On August 15, 2013, the Conspiracy used credentials harvested from the Outbrain spearphishing attack to obtain unauthorized access to Outbrain's advertising controls and was able to redirect web traffic for a number of Outbrain's customers including CNN, The Washington Post, and Time.

The Conspiracy Targets Chartbeat

83. On August 19, 2013, an email that appeared to be sent from the Chief Executive Officer of Chartbeat, Inc., was sent by a member of the Conspiracy to employees of Chartbeat. The email contained a link which appeared to resolve to a media website. However, the link actually resolved to http://deliveryroutes.co.uk/ch.php. An employee of Chartbeat (VICTIM 3) clicked on the link and entered her email login credentials. The Conspiracy also sent other phishing emails in an attempt to cause Chartbeat employees to click on malicious links.

84. On August 19, 2013, a member of the Conspiracy received an automated email at th3pr0123@gmail.com that included the credentials of VICTIM 3. Login data from VICTIM 3's email account show that a member of the Conspiracy logged into the account on August 19,

without authorization, using IP address 141.105.64.37 (which resolved to Russia). The same IP address was used to log into the email account leaks.syrian.es.org@gmail.com, a secondary account for th3pr0123@gmail.com.

85. Based on information from Chartbeat, VICTIM 3's email account contained the password for the Chartbeat Twitter account.

86. On August 21, 2013, a member of the Conspiracy accessed, without authorization, VICTIM 3's email account, using a computer associated with IP address 141.105.64.37. Using VICTIM 3's stolen credentials, the Conspiracy reset the password to a Chartbeat administrator account, which gave the Conspiracy access to some internal computer systems. On the same day, a member of the Conspiracy posted a message, without authorization, to a Chartbeat Twitter account that included a photograph and a reference to the Syrian Electronic Army.

The Conspiracy Targets USA Today

87. On August 20, 2013, an email appearing to be sent from an employee at Gannett was sent by a member of the Conspiracy to multiple Gannett employees with the subject line "News." A member of the Conspiracy had altered the email account so that it appeared to be sent from an actual Gannett employee and from the domain name "@gannett.com." The body of the email contained what appeared to be a link to a news article. However, the link actually directed the targets of the attack to a German website www.sws-schulen.de/gn.php that was associated with the Conspiracy, which prompted targets to provide their username and password.

88. On August 20, 2013, emails appearing to be from an employee at USA Today were sent by a member of the Conspiracy to multiple USA Today employees with the subject line "Breaking". The member of the Conspiracy altered the email account so that it appeared to

be sent from an actual USA Today employee and from the domain name "@usatoday.com." The body of the email contained what appeared to be a link to a news article. However, the link actually directed the targets of the attack to another German webpage used by the Conspiracy, www.sws-schulen.de/ut.php, which prompted the targets to provide their username and password.

The Conspiracy Targets the New York Times

89. On August 23, 2013, employees of Melbourne IT received an email sent by a member of the Conspiracy that appeared to come from the Chief Executive Officer of Melbourne IT. The email contained a malicious link. Two employees of Melbourne IT clicked on the link and entered system logon credentials.

90. On August 27, 2013, a member of the Conspiracy accessed, without authorization, Melbourne IT's computer systems using stolen credentials. The member of the Conspiracy searched through Melbourne IT's systems for information about Melbourne IT clients. A review of computer logs provided by Melbourne IT's corporate parent indicated that the IP address 82.137.250.235 was used by the member of the Conspiracy who compromised Melbourne IT's computer systems. Review of search warrant data indicates that the same IP address was used to log into the email account leaksyrianesorg@gmail.com six times between July 7, 2013, and August 11, 2013. In search warrant returns, leaks.syrianes.org@gmail.com was listed as an alternative account for the email address th3pr0123@gmail.com. Furthermore the same IP address was used to log into the account th3pr0123@gmail.com hundreds of times, including between August 23, 2013, and August 27, 2013. After logging into Melbourne IT's systems, a member of the Conspiracy redirected the domains for certain Melbourne IT clients,

including the New York Times, to a website controlled by the Conspiracy. The New York Times publicly reported that its website was down for a significant period of time.

The Conspiracy Targets the United States Marine Corps

91. On September 1, 2013, a member of the Conspiracy sent an email which appeared to come from the Chief Executive Officer of J. Walter Thompson (JWT), a company which provides services to the United States Marine Corps, to another employee of JWT. The subject line of the email was "News" and the email contained a link which appeared to resolve to a media website. In fact, the link resolved to www.kulalars.com/jwt.php. The JWT employee clicked on the link and was prompted to enter her credentials. The employee did so.

92. Shortly thereafter, a member of the Conspiracy used, without authorization, the employee's credentials to access her email account. The member of the Conspiracy then used the email account to request, by means of email, that JWT employee's Network Solutions password be reset. Network Solutions is a company that provides web-hosting and domain name services to the general public and JWT used Network Solutions to provide services to the Marines.com domain. The password reset link was sent to the employee's JWT email account. Using the employee's compromised credentials, a member of the Conspiracy reset the employee's Network Solutions password and deleted evidence of the password change from the employee's JWT email inbox. A member of the Conspiracy also created an email forwarding rule that caused all of the employee's emails to be forwarded to leaks.syrianes.org@gmail.com.

93. On September 2, 2013, a member of the Conspiracy altered, without authorization, an Internet-based recruiting site for the U.S. Marine Corps. The member of the Conspiracy logged into the employee's Network Solutions account and redirected the domain www.marines.com to a server controlled by the Conspiracy for approximately six hours. The

website to which the domain was redirected contained a message encouraging U.S. Marines to "refuse your orders" and inviting them to fight alongside the Syrian Army.

The Conspiracy Targets the National Aeronautics and Space Administration

94. Search warrant returns on the email account leakssyrianesorg@gmail.com indicate that on February 2, 2013, a member of the Conspiracy conducted Google searches for US and Israeli military and government webmail sites. During the searches, the member of the Conspiracy clicked on a link related to National Aeronautics and Space Administration's webmail domain.

95. On September 20, 2013, a member of the Conspiracy sent an email appearing to originate from an employee of the National Aeronautics and Space Administration (NASA) to twenty-six email addresses associated with actual employees at NASA facilities, including five email addresses associated with real persons working at NASA's Langley Research Center in Hampton, Virginia, which is in the Eastern District of Virginia. The email had the subject "News" and contained a link that appeared to point to a news article but actually directed to the domain http://karisdiscounts.com/nasa.php. In search warrant returns for the seatheshadow@gmail.com account, links to other phishing pages used by the Conspiracy and hosted at the htttp://karisdiscounts.com domain were located.

96. On September 20, 2013, four NASA employees, including a NASA Program Analyst at Langley Research Center in the Eastern District of Virginia, clicked on the link provided by a member of the Conspiracy. However, these employees were not able to access the domain because their attempts to visit it were stopped by NASA network security devices.

CONCLUSION

97. Based on the foregoing, I request the Court issue the attached complaint and arrest warrants.

Respectfully submitted,

Patrick DiMauro
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on June 12, 2014:

/s/Thomas Rawles Jones, Jr.
HON. T. RAWLES JONES, JR.
UNITED STATES MAGISTRATE JUDGE

Reviewed by
AUSAs Jay V. Prabhu & Andrew Peterson